**IN THE CLAIMS**

Please substitute claims 1-40 with the following:

1-20. (Canceled)

21. (Currently Amended) A person authentication method for executing person authentication by comparing a template which is person identification data acquired beforehand with sampling information input by a user, said method comprising the steps of:

acquiring an encrypted template from a person identification certificate including said template and generated by a third-party agency serving as a person identification certificate authority;

receiving said encrypted template from said person identification certificate authority and an encrypted sampling information from said user;

decrypting said encrypted template and said encrypted sampling information;

comparing said decrypted template with said decrypted sampling information, and

executing person authentication on the basis of the acquired template;

wherein,

said encrypted sampling information is generated using a public key certificate generated by a certificate authority; and

when transmitting said person identification certificate to ~~said~~ a person authentication system, said person identification certificate authority

(a) retrieves a stored encrypted template,

(b) decrypts the stored encrypted template using a private key of the person identification certificate authority,

(c) re-encrypts the decrypted template using a public key of said person authentication system to which said person identification certificate is to be transmitted, and

(d) stores the re-encrypted template in said person identification certificate.

22. (Original) A person authentication method according to Claim 21, wherein said person identification certificate authority writes a digital signature on the person identification certificate issued by said person identification certificate authority.

23. (Original) A person authentication method according to Claim 21, wherein said person identification certificate authority verifies the identification of a person requesting a person identification certificate to be issued, acquires a template serving as person identification data of said person requesting the person identification certificate to be issued, and generates a person identification certificate storing template information including said template.

24. (Previously Presented) A person authentication method according to Claim 21, wherein, in the process of acquiring the person identification certificate from said person identification certificate authority, said person authentication system performs mutual authentication between said person authentication system and said person identification certificate authority, and said person identification certificate authority transmits the person identification certificate, provided that said mutual authentication is successfully completed.

25. (Original) A person authentication method according to Claim 21, wherein said person identification certificate authority stores said template in said person identification certificate after encrypting said template.

26. (Canceled)

27. (Previously Presented) A person authentication method according to Claim 21, wherein said person authentication system is a service provider which makes a deal with a user identified by said person identification certificate, and

wherein said service provider compares a template, which is acquirable from a person identification certificate acquired from said person identification certificate authority, with sampling information provided by the user, and starts making a deal with the user, provided that said template and said sampling information match with each other.

28. (Previously Presented) A person authentication method according to Claim 21, wherein said person authentication system is a user device serving as a data processing apparatus including data accessible by a user identified by said person identification certificate, and

wherein said user device compares a template, which is acquirable from a person identification certificate acquired from said person identification certificate authority, with sampling information provided by the user, and said user device allows the user to start accessing said user device, provided that said template and said sampling information match with each other.

29. (Currently Amended) A person authentication method for executing person authentication by comparing a template which is a person identification data acquired beforehand with sampling information input by a user, comprising receiving, at a person identification certificate authority which acquires an encrypted template from a person identification certificate including said encrypted template, said encrypted template from said person identification certificate authority and an encrypted sampling information from said user; decrypting said encrypted template and said encrypted sampling information, and executing person authentication by comparing said decrypted template with said decrypted sampling information, wherein a verification certificate is issued provided that said person authentication is successfully passed; wherein said encrypted sampling information is generated using a public key certificate generated by a certificate authority; and wherein, when transmitting said person identification certificate to ~~said~~ a person authentication system, said person identification certificate authority retrieves a stored encrypted template, decrypts the stored encrypted template using a private key of the person identification certificate authority, re-encrypts the decrypted template using a public key of said person authentication system to which said person identification certificate is to be transmitted, and stores the re-encrypted template in said person identification certificate.

30. (Original) A person authentication method according to Claim 29, wherein said person identification certificate authority writes a digital signature on the verification certificate issued by said person identification certificate authority.

31. (Original) A person authentication method according to Claim 29, wherein said person identification certificate authority verifies the identification of a person requesting a person identification certificate to be issued, acquires a template serving as person identification data of said person requesting the person identification certificate to be issued, and generates a person identification certificate storing template information including said template.

32. (Previously Presented) A person authentication method according to Claim 29, wherein, in the process of acquiring said verification certificate from said person identification certificate authority, said person authentication system performs mutual authentication between said person authentication system and said person identification certificate authority, and said person identification certificate authority transmits the verification certificate, provided that said mutual authentication is successfully completed.

33. (Previously Presented) A person authentication method according to Claim 29, wherein said person authentication system acquiring the verification certificate is a service provider which provides services to an user, and

wherein said service provider starts providing services to the user, provided that the verification certificate is successfully acquired from said person identification certificate authority.

34. (Previously Presented) A person authentication method according to Claim 29, wherein said person authentication system acquiring the verification certificate is a user device serving as a data processing apparatus including data accessible by an user, and

wherein said user device allows the user to start accessing said user device, provided that the verification certificate is successfully acquired from said person identification certificate authority.

35. (Previously Presented) A person authentication method according to Claim 29, wherein said person authentication system verifies the signature of said verification certificate acquired from said person identification certificate authority and deletes said verification certificate after confirming that said verification of the signature indicates the validity of said verification certificate.

36-40. (Canceled)